

REMARKS

In the Office Action dated February 9, 2007, the Examiner indicated that claims 1-20 were rejected. Claims 1-20 remain pending in the application. Reconsideration of this application is respectfully requested.

Rejections – 35 U.S.C. § 103

1. Rejection of claims 1, 10-12, and 15-20

Claims 1, 10-12, and 15-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,618,807 (“*Wang*”) in view of U.S. Patent No. 7,111,324 (“*Elteto*”). Applicants respectfully submit that *Wang* and *Elteto*, alone or in combination, fail to teach or disclose various claimed limitations of claims 1, 10-12, and 15-20. Further, a skilled artisan at the time of the invention would not have combined *Wang* with any other reference cited by the Examiner to arrive at the claimed invention.

Independent Claim 1

It is respectfully submitted that independent claim 1 is allowable over *Wang* in view of *Elteto*, because these references, alone or in combination, fail to disclose or teach, among other things, (1) a first storage unit to store an authentication sequence; (2) a read-only memory unit to store an authentication algorithm; (3) a microcontroller coupled to said first storage unit, said read-only memory unit, and a web server, wherein said microcontroller is to receive said password and execute said authentication algorithm and wherein said authentication algorithm is to verify said password with said authentication sequence; and (4) a second storage unit coupled to said microcontroller to store data from said web server and wherein access to said second storage unit is permitted by said microcontroller only if said password has been verified, wherein the system is arranged to receive data from the web server, via the host, in encrypted form and to decrypt that data before use thereof in the host.

Wang does not teach a system with a read-only memory unit that stores an authentication algorithm. *Wang* discloses a system in which the “system memory” stores a cryptoprogram (see Figure 1 [block 18], column 2, lines 7, 40-42). A cryptoprogram stored in the system memory is not an authentication algorithm stored in the read-only memory. A skilled artisan at the time of the invention would have understood that the contents of the system memory in a computer system can be easily altered (and hence the cryptoprogram stored in such system memory may be easily altered). Therefore, Applicants respectfully submit that *Wang* does not teach or disclose this claim limitation of claim 1. It would not have been obvious to a skilled artisan at the time of the invention to add a separate read-only memory unit in addition to the system memory to store an authentication algorithm.

Wang does not disclose the use of a microcontroller to execute an authentication algorithm stored in a read-only memory. Therefore, Applicants respectfully submit that *Wang* does not teach or disclose this claim limitation of claim 1. It would not have been obvious to a skilled artisan at the time of the invention to use a microcontroller to execute an authentication algorithm stored in a read-only memory.

Wang does not teach a system which uses an authentication algorithm to verify the password with the authentication sequence. *Wang* discloses a system wherein a received password is matched to a stored password without the execution of an authentication algorithm (stored in a read-only memory) to verify the password with the authentication sequence (column 2, lines 42-50). Applicants therefore respectfully submit that *Wang* does not teach or disclose this claim limitation of claim 1. It would not have been obvious to a skilled artisan at the time of the invention to execute an authentication algorithm (stored in a read-only memory) to verify the password with an authentication sequence.

The Examiner argues that system memory 20 in *Wang* discloses the limitation of the read-only memory unit to store an authentication algorithm in the present invention, yet at the same time the Examiner argues that system memory 20 in *Wang* also discloses the limitation of the second storage unit coupled to the microcontroller to store data from the web server in the present invention. Applicants respectfully submit that system memory 20 in *Wang* does not and cannot concurrently disclose a read-only memory unit and a separate second storage unit.

In addition, the Examiner argues that the electronic key with programmable memory 28 in *Wang* discloses the limitation of the first storage unit to store an authentication sequence in the present invention, yet at the same time the Examiner argues that programmable memory 28 in *Wang* also discloses the limitation of the second storage unit coupled to the microcontroller to store data from the web server in the present invention. Applicants respectfully submit that programmable memory 28 in *Wang*'s electronic key does not and cannot concurrently disclose a first storage unit and a separate second storage unit.

Furthermore, *Wang* does not teach a second storage unit coupled to the microcontroller to store data from the web server and wherein access to second storage unit is allowed by the microcontroller only if the password has been verified. Rather, all *Wang* discloses is a cryptoprogram that decrypts files stored in the system memory (Figure 1 [block 20], column 2, lines 3-4, column 2, lines 44-45). The "act" of decrypting files stored in the system memory is different from a separate second storage unit itself. Applicants therefore respectfully submit that *Wang* does not teach or disclose this claim limitation of claim 1.

The Examiner agrees that *Wang* does not teach a system wherein the system be arranged to receive data from the web server, via the host, in encrypted form and to decrypt that data before use thereof in the host. The Examiner cites *Elteto* as teaching a system wherein data is

received from a web server, via the host. Applicants respectfully disagree. *Elteto* teaches a system used to control access to remote servers (column 4, lines 35-62). *Elteto* does not teach receiving data from the web server via a host or storing data from the web server into a second storage unit. Applicants therefore respectfully submit that *Elteto* does not teach or disclose this claim limitation of claim 1.

Independent Claim 18

It is respectfully submitted that independent claim 18 is allowable over *Wang* in view of *Elteto*, because these references, alone or in combination, fail to disclose or teach, among other things, a method for authenticating a password, comprising: (1) coupling an authentication system to a host for communication therewith; (2) the system receiving said password; (3) the system receiving data from a web server, via the host, in encrypted form, wherein said data is stored in a storage unit of the system; (4) the system providing an authentication sequence; (5) the system executing an authentication algorithm to verify said password with said authentication sequence, wherein said authentication algorithm is stored on a read-only memory unit of the system; (6) the system permitting access to said data on said storage unit only if said password is verified; and (7) the system decrypting the data before use in the host.

The Examiner agrees that *Wang* does not disclose a system receiving data from a web server, via the host, in encrypted form, wherein the data is stored in a storage unit. The Examiner cites *Elteto* as teaching a system receiving data from a web server, via the host, in encrypted form, wherein the data is stored in a storage unit. Applicants respectfully disagree. *Elteto* teaches a system controlling access to remote servers (column 4, lines 35-62). *Elteto* does not teach a system receiving data from the web server via a host or storing data from the web

server into a second storage unit. Applicants therefore respectfully submit that *Elteto* does not teach or disclose this claim limitation of claim 18.

Wang does not teach the system providing an authentication sequence. A system storing a password is not a system providing an authentication sequence. Applicants therefore respectfully submit that *Wang* does not teach or disclose this claim limitation of claim 18.

Wang does not teach the system executing an authentication algorithm to verify the password with the authentication sequence, wherein such authentication algorithm is stored on a read-only memory unit. *Wang* teaches the cryptoprogram searching for a stored password to be matched with a received password, wherein the cryptoprogram is stored in the system memory of which the contents can be easily altered, as opposed to a separate read-only memory unit. In addition, matching a stored password with a received password is not executing an authentication algorithm to verify the password with the authentication sequence. Applicants therefore respectfully submit that *Wang* does not teach or disclose this claim limitation of claim 18.

Wang does not teach the use of a read-only memory unit to store an authentication algorithm. *Wang* discloses a system wherein a cryptoprogram, stored in system memory, searches the programmable memory in an electronic key for a password (Figure 1 [block 18], column 2, lines 7, 40-42). Using the read-only memory unit to store an authentication algorithm is different from using the system memory to store a cryptoprogram stored because the contents of system memory can be easily altered (and hence the cryptoprogram stored in such system memory may be easily altered). Therefore, Applicants respectfully submit that *Wang* does not teach or disclose this claim limitation of claim 18.

Wang does not disclose a system permitting access to data on the storage unit only if the password is verified with the authentication sequence. Rather, *Wang* discloses a system in which

a cryptoprogram decrypts files stored in the system memory after the password is matched (Figure 1 [block 20], column 2, lines 3-4, column 2, lines 44-45). *Wang* permits “access” to the files in the system memory even before the password is matched, although at that point the files are still encrypted (but themselves accessible nonetheless). Applicants therefore respectfully submit that *Wang* does not teach or disclose this claim limitation of claim 18.

Dependent Claims 10-12, 15-17, 19, and 20

Dependent claims 10-12, 15-17, 19, and 20, each being dependent on one of independent claims 1 and 18, are deemed allowable for the same reasons expressed above with respect to independent claims 1 and 18.

Regarding claim 10, *Wang* does not disclose an encoder coupled between the microcontroller and the second storage unit, wherein the encoder is to encrypt data that is to be written onto the second storage unit. The Examiner cites column 1, lines 35-36, and column 2, lines 29-38 of *Wang* and argues that *Wang* teaches the use of an encoder between the microcontroller and the second storage unit. Applicants respectfully disagree. *Wang* teaches the use of a cryptoprogram to encrypt data stored in the system memory (column 2, lines 3-4, column 2, lines 29-38). A cryptoprogram itself stored in the system memory to encrypt data also stored in the system memory is not an encoder coupled between the microcontroller and the second storage unit. Applicants therefore respectfully submit that *Wang* does not disclose or teach claim 10 of the present invention.

Regarding claim 11, *Wang* does not disclose a decoder coupled between the microcontroller and the second storage unit, wherein the decoder is to decrypt data that is to be read from the second storage unit. The Examiner cites column 1, lines 35-36, and column 2, lines 44-53 of *Wang* and argues that *Wang* teaches the use of a decoder between the

microcontroller and the second storage unit. Applicants respectfully disagree. *Wang* teaches the use of a cryptoprogram to decrypt data stored in the system memory (column 2, lines 3-4, column 2, lines 29-37). A cryptoprogram itself stored in the system memory to decrypt data also stored in the system memory is not a decoder coupled between the microcontroller and the second storage unit. Applicants therefore respectfully submit that *Wang* does not disclose or teach claim 11 of the present invention.

Regarding claim 12, *Elteto* does not disclose a system wherein data stored in the second storage unit is hash-coded. The Examiner cites column 8, lines 19-39 of *Elteto* and argues that *Elteto* discloses a system wherein data stored in the second storage unit is hash coded. Applicants respectfully disagree. *Elteto* discloses a system wherein hashing is used for message authentication, not data storage. In other words, *Elteto* does not teach hash-coding the stored data. Applicants respectfully submit that *Elteto* does not teach or disclose claim 12 of the present invention.

Regarding claim 15, *Wang* does not disclose a system wherein the first storage unit is located in the read-only memory unit and wherein the authentication sequence is hard coded into the first storage unit. The Examiner cites column 2, lines 14-28 of *Wang* and argues that *Wang* teaches a system wherein the first storage unit is located within the read-only memory unit and wherein the authentication sequence is hard coded into the first storage unit. Applicants respectfully disagree. *Wang* does not teach the use of read-only memory for the storage of the authentication sequence. *Wang* specifically teaches the storage of a password in the programmable memory of an electronic key (Figure 1 [block 18], column 2, lines 14-28). Storing a password in programmable memory is not hard-coding an authentication sequence into read-only memory because a password stored in programmable memory can be easily altered

and/or erased. Therefore, Applicants respectfully submit that *Wang* does not teach or disclose claim 15 of the present invention.

Regarding claim 16, *Elteto* does not disclose a system wherein the second storage area comprises a public storage area and a private storage area. The examiner cites Figure 3 [block 324] and Figure 3 [block 326] of *Elteto* and argues that *Elteto* teaches the system wherein the second storage area comprises a public storage area and a private storage area. *Elteto* discloses the use of a processor operation program instruction space and an auxiliary program instruction space. These instruction spaces relate to processor operation instructions as opposed to areas for storage (column 7, lines 20-37). Furthermore, the instruction spaces disclosed in *Elteto* relate to the electronic key itself as opposed to a secondary storage area (column 7, lines 20-37). Applicants therefore respectfully submit that *Elteto* does not teach or disclose claim 16 of the present invention.

Regarding claim 17, the Examiner agrees that *Wang* and *Elteto* do not teach the system wherein first storage unit is located within the private storage area of the second storage area. However, the Examiner argues that locating the first storage area within the private storage area of the second storage area would have been obvious to the skilled artisan at the time of the invention. Applicants respectfully disagree. Locating the first storage unit within the private storage area of the second storage area provides an advantage in that it makes it more difficult for an unauthorized user to access or modify the first storage area. This would not have been obvious to a person of ordinary skill in the art at the time of the invention. Applicants therefore respectfully submit that claim 17 would not have been obvious to a person of ordinary skill in the art at the time of the invention.

Regarding claim 19, *Elteto* does not teach a system wherein the password is received from the web server. The Examiner cites column 7, lines 37-49 of *Elteto* and argues that *Elteto* teaches a system wherein the password is received from the web server. Applicants respectfully disagree. *Elteto* discloses a system where a key is supplied to remotely located employees (column 7, lines 40-43). However, *Elteto* does not disclose how to accomplish the key supply. Applicants therefore respectfully submit that *Elteto* does not teach claim 19 of the present invention.

2. Rejection of Dependent Claims 2-9 and 13

Dependent claims 2-9 and 13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Wang* in view of *Elteto*, and further in view of U.S. Patent No. 6,038,320 ("*Miller*").

Dependent claims 2-9 and 13, each being dependent on independent claim 1, are deemed allowable for the same reasons expressed above with respect to independent claim 1.

Regarding claim 2, *Miller* does not disclose the system wherein the password is received by the microcontroller from the host. The Examiner cites column 5, lines 54-64 of *Miller* and argues that *Miller* teaches a system wherein the password is received by the microcontroller by the host. Applicants respectfully disagree. *Miller* does not specifically teach the receipt of a password by a microcontroller from a host. Applicants respectfully submit that *Miller* does not teach or disclose claim 2 of the present invention.

Regarding claim 3, *Miller* does not teach the system wherein the read-only memory unit further comprises a shutdown algorithm to shut down the host and the authentication system after a number of incorrect passwords is received by the microcontroller. The Examiner cites *Miller*

Figure 8 [block 300], column 5, lines 1-9, and column 5, lines 53-64 and argues that *Miller* teaches a shutdown algorithm. Applicants respectfully disagree. *Miller* teaches a system where authentication is required to wake a computer from sleep mode (column 5, lines 36-63).

Waking a computer from sleep mode is different from shutting down a host whose operating system is currently running. Applicants therefore respectfully submit that *Miller* does not teach this claim limitation of claim 3.

Regarding claim 4, *Elteto* does not disclose a system wherein the password is received by the host from the web server. The Examiner cites column 7, lines 37-49 of *Elteto* and argues that *Elteto* teaches a system where the password is received by the host from the web server. Applicants respectfully disagree. *Elteto* discloses a system where a personal key is supplied to remotely located employees (column 7, lines 40-43). However, *Elteto* does not disclose how to accomplish the personal key supply. Applicants therefore respectfully submit that *Elteto* does not teach this claim limitation of claim 4.

Regarding claim 5, *Wang* does not teach the system wherein the authentication algorithm is hard coded on one of a group consisting of a firmware and a hardware in the microcontroller. The Examiner cites column 2 lines 1-14 of *Wang* and argues that *Wang* teaches a system where the authentication algorithm is hard coded. Applicants respectfully disagree and note that *Wang* specifically discloses the use of a cryptoprogram stored in the system memory (Figure 1 [block 26], column 2, line 7). Storing a cryptoprogram in system memory is different from hard-coding an algorithm into firmware or hardware, because a program stored in system memory can be easily altered. Applicants respectfully submit that *Wang* does not teach or disclose claim 5.

Regarding claims 6 and 7, *Wang* does not teach the system wherein the second storage unit is a removable storage device. *Wang* does not teach the system wherein the second storage

unit uses flash memory. The Examiner cites column 2, lines 14-28 of *Wang* and argues that *Wang* teaches a system wherein the second storage unit is a removable storage device. Applicants respectfully disagree. *Wang* teaches a system where the electronic key is a removable portable device (column 2, lines 14-28). However, *Wang* does not disclose a system wherein the electronic key is used for storage. *Wang* discloses a system where the key is used to store a password only. *Wang* discloses a system where data storage occurs in the system memory of the host computer (Figure 1 [block 20], column 2, lines 1-13). *Wang* does not disclose a system where the storage unit is a removable storage device. Applicants therefore respectfully submit that *Wang* does not teach or disclose claim 6 of the present invention. Further, *Wang* does not disclose the use of flash memory for data storage. Applicants therefore respectfully submit that *Wang* does not teach or disclose claim 7 of the present invention.

3. Dependent Claim 14

Dependent claim 14 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over *Wang* and *Elteto* and further in view of U.S. Patent No. 6,178,508 (“*Kaufman*”).

Dependent claim 14, being dependent on independent claim 1, is deemed allowable for the same reasons expressed above with respect to independent claim 1.


CONCLUSION

Applicants assert that all of the pending claims are patentable over the cited references. A favorable consideration of the original application is respectfully requested. If the Office desires a telephone conference, the undersigned can be reached at the number below.

Attached hereto is a petition for extension of time for three (3) months. In connection therewith, the Commissioner is hereby authorized to charge the fee required under 37 CFR § 1.136(a) to White & Case LLP Deposit Account No. 50-3672. Applicants are unaware of any other fees due at this time. However, if other fees are due for this extension or any other matter concerning this response, the Commissioner is authorized to charge the fees to the above-listed Deposit Account.

Respectfully submitted,

Dated: 8/9/2007



Warren S. Heit (Reg. No. 36,828)
White & Case LLP
1155 Avenue of the Americas
New York, NY 10036-2787
(650) 213-0300